CLAIMS

What is claimed is:

1. A method performed by a user terminal of a wireless access network, the method comprising:

generating a shared secret to be provided to an access point of the wireless access network;

encrypting the shared secret with an access point public key;

generating an authenticator string, the authenticator string demonstrating possession of a user terminal private key;

sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate, and the authenticator string.

2. The method of claim 1, wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

3. The method of claim 2, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point.

4. The method of claim 1, wherein generating the authenticator string comprises generating an authenticator message and signing the authenticator message with the user terminal private key.

5. The method of claim 4, wherein signing the authenticator message comprises:

generating a digest of the authenticator message; and

encrypting the authenticator message digest with the user terminal private key.

6. The method of claim 4, wherein the authenticator message comprises a time parameter and at least part of the shared secret.

7. The method of claim 6, wherein the user terminal generates the authenticator string by speculatively incrementing the time parameter to a time when the message is to be sent to the access point.

8. The method of claim 7, wherein the time parameter comprises and absolute frame number, and the user terminal speculatively increments the absolute frame number to be included in the authenticator message from the current absolute frame number to the absolute number of the frame in which the message is to be sent to the access point.

9. The method of claim 1, wherein the user terminal generates and encrypts the shared secret prior to identifying the access point by speculatively encrypting the shared secret with the public keys of a plurality of access points stored in the user terminal.

10. A method performed by an access point of a wireless access network, the method comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, a user terminal certificate, and an authenticator string demonstrating possession by the user terminal of a user terminal private key;

decrypting the shared secret using an access point private key;

authenticating the user terminal by checking the authenticator string using a user terminal public key included in the user terminal certificate to verify possession of the user terminal private key by the user terminal.

11. The method of claim 10, wherein the user terminal certificate is scrambled, and the access point unscrambles the user terminal certificate using the shared secret.

12. The method of claim 10, wherein checking the authenticator string comprises decrypting the authenticator string using the user terminal public key.

13. The method of claim 12, wherein checking the authenticator string further comprises generating an authenticator message, generating a digest of the authenticator message, and comparing the authenticator message digest with the decrypted authenticator string.

14. The method of claim 13, wherein the authenticator message comprises at least part of the shared secret.

15. The method of claim 10, wherein the user terminal certificate is signed by a certificate authority trusted by the access point.

16. The method of claim 10, wherein the shared secret is to be used for symmetric key cryptography between the access point and the user terminal.

17. A user terminal comprising:

a memory to store a user terminal certificate and a shared secret to be provided to an access point;

a processor coupled to the memory to encrypt the shared secret with an access point public key, and to generate an authenticator string demonstrating possession of a user terminal private key;

a transmitter coupled to the processor to send a message to the access point, the message including the encrypted shared secret, the user terminal certificate, and the authenticator string.

18. The user terminal of claim 17, wherein the processor is further to scramble the user terminal certificate using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

19. The user terminal of claim 18, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point.

20. The user terminal of claim 17, wherein the processor generates the authenticator string by generating an authenticator message and signing the authenticator message with the user terminal private key.

21. The user terminal of claim 20, wherein signing the authenticator message comprises:

generating a digest of the authenticator message; and

encrypting the authenticator message digest with the user terminal private key.

22. The user terminal of claim 20, wherein the authenticator message comprises a time parameter and at least part of the shared secret.

23. The user terminal of claim 22, wherein the processor generates the authenticator string by speculatively incrementing the time parameter to a time when the message is to be sent to the access point.

24. The user terminal of claim 23, wherein the time parameter comprises and absolute frame number, and the user terminal speculatively increments the absolute

frame number to be included in the authenticator message from the current absolute frame number to the absolute number of the frame in which the message is to be sent to the access point.

25. The user terminal of claim 17, wherein the memory is further to store public keys of a plurality of access points, and the processor generates and encrypts the shared secret prior to the user terminal identifying the access point by speculatively encrypting the shared secret with the public keys of the plurality of access points.

26. An access point comprising:

a receiver to receive a message from a user terminal, the message containing a shared secret encrypted by the user terminal with an access point public key, a user terminal certificate including a user terminal public key, and an authenticator string demonstrating possession by the user terminal of a user terminal private key corresponding with the user terminal public key; and

a processor coupled to the receiver to decrypt the shared secret using an access point private key, and to authenticate the user terminal by verifying possession by the user terminal of the user terminal private key.

27. The access point of claim 26, wherein the user terminal certificate is scrambled, and the processor is further to unscramble the user terminal certificate using the shared secret.

28. The access point of claim 26, wherein the processor verifies possession of the user terminal private key by decrypting the authenticator string using the user terminal public key.

29. The access point of claim 28, the processor further verifies possession of the user terminal private key by generating an authenticator message, generating a digest of the authenticator message, and comparing the authenticator message digest with the decrypted authenticator string.

30. The access point of claim 29, wherein the authenticator message comprises at least part of the shared secret.

31. The access point of claim 26, wherein the user terminal certificate is signed by a certificate authority trusted by the access point.

32. The access point of claim 26, wherein the shared secret is to be used for symmetric key cryptography between the access point and the user terminal.

33. A machine-readable medium storing data representing instructions that, when executed by a processor of a user terminal, cause the processor to perform operations comprising:

generating a shared secret to be provided to an access point of the wireless access network;

encrypting the shared secret with an access point public key;

generating an authenticator string, the authenticator string demonstrating possession of a user terminal private key;

sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate, and the authenticator string.

34. The machine-readable medium of claim 33, wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

35. The machine-readable medium of claim 34, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point.

36. The machine-readable medium of claim 33, wherein generating the authenticator string comprises generating an authenticator message and signing the authenticator message with the user terminal private key.

37. The machine-readable medium of claim 36, wherein signing the authenticator message comprises:

generating a digest of the authenticator message; and

encrypting the authenticator message digest with the user terminal private key.

38. The machine-readable medium of claim 36, wherein the authenticator message comprises a time parameter and at least part of the shared secret.

39. The machine-readable medium of claim 38, wherein the user terminal generates the authenticator string by speculatively incrementing the time parameter to a time when the message is to be sent to the access point.

40. The machine-readable medium of claim 39, wherein the time parameter comprises and absolute frame number, and the user terminal speculatively increments the absolute frame number to be included in the authenticator message from the current absolute frame number to the absolute number of the frame in which the message is to be sent to the access point.

41. The machine-readable medium of claim 33, wherein the user terminal generates and encrypts the shared secret prior to identifying the access point by speculatively

encrypting the shared secret with the public keys of a plurality of access points stored in the user terminal.

42. A machine-readable medium storing data representing instructions that, when executed by a processor of an access point, cause the processor to perform operations comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, a user terminal certificate, and an authenticator string demonstrating possession by the user terminal of a user terminal private key;

decrypting the shared secret using an access point private key;

authenticating the user terminal by checking the authenticator string using a user terminal public key included in the user terminal certificate to verify possession of the user terminal private key by the user terminal.

43. The machine-readable medium of claim 42, wherein the user terminal certificate is scrambled, and the access point unscrambles the user terminal certificate using the shared secret.

44. The machine-readable medium of claim 42, wherein checking the authenticator string comprises decrypting the authenticator string using the user terminal public key.

45. The machine-readable medium of claim 44, wherein checking the authenticator string further comprises generating an authenticator message, generating a digest of the authenticator message, and comparing the authenticator message digest with the decrypted authenticator string.

46. The machine-readable medium of claim 45, wherein the authenticator message comprises at least part of the shared secret.

47. The machine-readable medium of claim 42, wherein the user terminal certificate is signed by a certificate authority trusted by the access point.

48. The machine-readable medium of claim 42, wherein the shared secret is to be used for symmetric key cryptography between the access point and the user terminal.